



COMPUTER USER AGREEMENT

284th BASE SUPPORT BATTALION INFORMATION MANAGEMENT



As a user of a USAREUR automated information system, I will adhere to the following security rules:

1. I will use Army information systems (computers, systems, and networks) only for authorized purposes.
2. I will not import any Government-owned software or install hardware on any Government-owned computer (for example, client-workstation, server) without first getting written approval from my system administrator (SA) or information systems security officer (ISSO).
3. I will not try to access data or use operating systems or programs, except as specifically authorized.
4. I know I will be issued a user identifier and a password to authenticate my computer account. After receiving them—
 - a. I will not allow anyone else to have or use my password. If I know that my password has been compromised, I will report to my SA for a new one.
 - b. If my account is on a classified network, I understand that my password is classified at the highest level of information in that network, and I will protect it in the same manner as that information.
 - c. I am responsible for all activity that occurs on my individual account once my password has been used to log on, as long as I am the sole user of the account and the account is protected by a password that is known only by me.
 - d. If I have a classified account, I will ensure that my password is changed at least once every 3 months or when compromised, whichever is sooner.
 - e. If I have an unclassified account, I will ensure that my password is changed at least twice a year or when compromised, whichever is sooner.
 - f. I understand that if my password does not meet current USAREUR standards (for example, length, character set, no prohibited sequences or combinations), I am to inform the SA.
 - g. I will not store my password on any processor or microcomputer or on any magnetic or electronic media unless approved in writing by the ISSO.

h. I will not tamper with my computer to avoid adhering to USAREUR password policy.

i. I will never leave my classified computer unattended if it is a classified system while I am logged on or while the computer is unprotected by a “password protected” screensaver.

5. I know that it is a violation of policy for any computer user to try to mask or hide his or her identity, or to try to assume the identity of someone else.

6. I know that if connected to the Secure Data Network (SDN), my system operates at least in the U.S. Secret, “system-high” mode.

a. Any magnetic media used on the system must be immediately classified and protected at the system-high level, regardless of the implied classification of the data (until declassified or downgraded by an approved process). In other words, any disk going into a Secret system is now Secret and must be handled accordingly.

b. I must protect all material printed out from the SDN at the system-high level until I or someone with the appropriate clearance personally reviews and properly classifies the material.

c. I will not enter information into a system if the information has a higher classification than that for which the system is rated. I will not enter information that is proprietary, contractor-excluded, or otherwise needs special protection or handling, unless approved in writing by the ISSO.

d. If connected to the SDN, only U.S. personnel with a security clearance are allowed unescorted access to the system.

e. Magnetic disks or diskettes will not be removed from the computer area without the approval of the local commander or head of the organization.

7. My local ISSO has informed me of TEMPEST (Red/Black) separation requirements for system components, and I will ensure that those requirements are met. I will not move hardware or alter communications connections without first getting approval from the SA or ISSO.

8. I will check all magnetic media for malicious software (that is, viruses) before loading it onto a USAREUR system or network.

9. I will not forward chain-mail or virus warnings. (The Regional Computer Emergency Response Team, Europe, issues virus alerts and threat advisories.) I will report chain-mail or virus warnings to my ISSO and delete the message. I will not attempt to run “sniffer” or other hacker-related software on the system.

10. I know I am subject to disciplinary action for any abuse of access privileges.

11. If I observe anything on the system I am using that indicates inadequate security, I will immediately notify the site ISSO. I know what constitutes a security incident and know that I must immediately report such incidents to the ISSO.

12. I will comply with security guidance issued by my system administrator and ISSO.

I understand this agreement and will keep the system secure. If I am the site supervisor, group chief, SA, or ISSO, I will ensure that all users in my area of responsibility sign this agreement.

User's Signature
Date

IMO's Signature
Name
Date

Security Officer's Signature
Name
Date